For Official Use Only

When Filled In

C01 PDL Summary Report

PDL:	Traditional DOD - Traditional Review for DOD sites	**Discrepancy Group:**	PDI-Traditional - Traditional
Default Additional Considerations:			

17 September 2004

Screen Sort Order:	CS - 010	**Report Sort Order:**	CS - 010	**PDI Key**	5449
Short Description Identifier:	CS - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	The COMSEC account is not managed in accordance with NSA or Service Standards.				
Default Severity:	Category II			**Category:**	16K-COMSEC Accounting
Reference:	NSA Manual 90-2				
Default Vulnerability Discussion:	Improper COMSEC account management can result in the loss or compromise of classified cryptologic devices or key.				
Default Finding Details:					
Default Recommendation:	Ensure that a person has been identified to be either the COMSEC custodian or Hand Receipt Holder. (NSA Manual 90-2, paragraph 3001) Ensure that COMSEC material is stored in a GSA approved container such as safe, vault, or secure room. (NSA Manual 90-2, paragraphs 6005, and 14002)				
Supplemental Information:	Level 1 Certification SIPRNet Compliance Validation				

Screen Sort Order:	CS - 020	**Report Sort Order:**	CS - 020	**PDI Key**	5450
Short Description Identifier:	CS - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	COMSEC briefings are not being given to COMSEC users.				
Default Severity:	Category III			**Category:**	13-Training
Reference:	NSA Manual 90-2, Chapter 6, Sec 6012				
Default Vulnerability Discussion:	Failure to properly brief COMSEC user could result in the loss of cryptologic devices or key, or the compromise of classified information.				
Default Finding Details:					
Default Recommendation:	Ensure that users have the appropriate clearance, need-to-know, and are aware of the physical security measures necessary to protect the material.				
Supplemental Information:					

Screen Sort Order:	CS - 040	**Report Sort Order:**	CS - 040	**PDI Key**	5453
Short Description Identifier:	CS - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	A Protected Distribution System (PDS) is required, however it has not been approved by the cognizant authority, and/or it is not constructed, configured, inspected, monitored and maintained in accordance with established requirements/guidelines.				
Default Severity:	Category I			**Category:**	16-Network and Communications Security
Reference:	NSTISSI 7003				
Default Vulnerability Discussion:	A PDS that is not approved or that is not constructed, configured, inspected, monitored and maintained as required could result in the interception of classified information.				
Default Finding Details:					
Default Recommendation:	1. Ensure that classified circuits exiting a control space is either encrypted or secured in an approved PDS. 2. If the classified circuits are secured in a PDS, ensure that the PDS is approved by the cognizant authority and constructed, configured, inspected, monitored and maintained as follows: a. The PDS is approved for use by the approving authority. NSTISSI 7003, para 8. b. The PDS terminal equipment is in a controlled area. NSTISSI 7003, Annex B para 1a(1). c. Periodic visual inspections are conducted as required. NSTISSI 7003, Annex B para 1a(6). d. The PDS lines are in full view of personnel conducting required inspections. NSTISSI 7003, Annex B para 1a(2). e. Records of inspection are being maintained. NSTISSI 7003, Annex B para 1a(4). f. Personnel are aware that the PDS exists; they have been trained to conduct inspections and report any suspicious activity. NSTISSI 7003, Annex B para 1a(3). g. Hardened carriers will be constructed as follows: NSTISSI 7003, Annex B para 4a. 1. Data cables must be installed in a carrier constructed of electrical metallic tubing (EMT), ferrous conduit or pipe, or rigid-sheet steel ducting, utilizing elbows, couplings, nipples and connectors of the same material. 2. The PDS pull boxes (if used): (a) The covers are sealed at mating surfaces. (b) The hinge pins are non-removable. (c) The box is secured with a GSA approved changeable combination padlock. 3. The PDS connections are permanently sealed surfaces (welding, compression, epoxy, fusion, etc). 4. If the PDS is buried, it is at least 1 meter below the surface (CONUS or US government owned or leased property). 5. Access manholes should be secured with a GSA approved changeable combination lock or a standard locking manhole cover with micro-switch alarms. 6. Suspended systems between buildings should be elevated a minimum of 5 meters above the ground and only used if the property traversed is owned or leased by the US government. h. Simple carriers will be constructed as follows: NSTISSI 7003, Annex B para 4b. 1. Data cables should be installed in a carrier constructed of any material (wood, PVC, EMT, ferrous conduit.				

	2. Joints and access points should be secured and controlled by personnel cleared to the highest level of data handled by the PDS.
Supplemental Information:	SIPRNet Compliance Validation Level 1 Checklist

---

Screen Sort Order:	CS - 050	**Report Sort Order:**	CS - 050	**PDI Key**	5454
Short Description Identifier:	CS - 050			**Process Status:**	Production
External System ID:					
PDI Short Description:	Protection of controlled unclassified information during transmission is not utilizing DES or another method meeting the requirements of FIPS 140.				
Default Severity:	Category III			**Category:**	16J-Encryption Devices
Reference:	DODD C-5200.5, para D.1; FIPS 140				
Default Vulnerability Discussion:	Failure to protect controlled unclassified information can result in its inadvertent release to unauthorized personnel.				
Default Finding Details:					
Default Recommendation:	Ensure controlled unclassified information is properly protected during transmission.				
Supplemental Information:	Level 1				

Screen Sort Order:	CS - 060	**Report Sort Order:**	CS - 060	**PDI Key**	5555
Short Description Identifier:	CS - 060			**Process Status:**	Production
External System ID:					
PDI Short Description:	All users of official DoD telephones and telephone systems subject to monitoring have not received adequate notice that their use of such telephones and telphone systems constitutes consent to COMSEC telephone monitoring.				
Default Severity:	Category III			**Category:**	22-Security Monitoring
Reference:	DODD 4640.6, para 6.1				
Default Vulnerability Discussion:	Failure to inform personnel of the proper use of government telephones or telephone systems could result in a classified discussion being conducted over an unclassified telephone. Failure to inform personnel of monitoring could affect the prosecution of personel caught intentionally or unintentionally discussing classified information on an unclassified telephone.				
Default Finding Details:					
Default Recommendation:	Using one of the following methods ensure all users of official DoD telephones and telephone systems are made aware that such telephones and telphone systems are subject to monitoring. a. Decals (DD Form 2056) attached to telephones subject to COMSEC telephone monitoring (required in DISA). b. A notification and consent form. c. Special memoranda from responsible senior officials. d. Initial briefing of new personnel and periodic rebriefings. e. Periodic notices in daily bulletins and similar publications. f. Any other means approved by the General Counsel of the Component concerned.				

Supplemental Information:	

Screen Sort Order:	FN - 010	**Report Sort Order:**	FN - 010	**PDI Key**	5455
Short Description Identifier:	FN - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	Organizations that have foreign nationals assigned have not adequately informed civilians, military and contractors of the limitations on access to information by foreign nationals and their unique responsibilities in working and dealing with them.				
Default Severity:	Category I			**Category:**	13F-Workforce Security Training
Reference:	DODD 5230.20, para 4.9.3				
Default Vulnerability Discussion:	Failure to properly inform all civilians, military and contractors of limitations could result in an inadvertent release of sensitive or classified information to foreign nationals.				
Default Finding Details:					
Default Recommendation:	All civilians, military and contractors who work in an organization that has foreign nationals assigned must be informed of the limitations on access to information by foreign nationals. An SOP should be developed detailing the responsibilities of civilians, military and contractors when working and dealing with foreign nationals.				
Supplemental Information:	SIPRNet Compliance Visit				

Screen Sort Order:	FN - 020	**Report Sort Order:**	FN - 020	**PDI Key**	5456
Short Description Identifier:	FN - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	Foreign nationals assigned to the command are not issued badges or passes that clearly identify them as foreign nationals. Proper guidelines are not being followed when the badges or passes are issued.				
Default Severity:	Category II			**Category:**	15C-Badges/ID
Reference:	DODD 5230.20, para 4.12 and 4.13				
Default Vulnerability Discussion:	Failure to properly identify foreign nationals could lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Ensure foreign nationals are issued badges or passes that clearly identify them as foreign nationals and the badges or passes are issued according to proper guidelines.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	FN - 030	**Report Sort Order:**	FN - 030	**PDI Key**	5457
Short Description	FN - 030			**Process Status:**	Production

Identifier:	
External System ID:	
PDI Short Description:	Foreign Liaison Officers (FLOs) are not required to wear their own countrys uniform with their badge or pass identifying them as foreign nationals in clear view.
Default Severity:	Category II
Category:	15C-Badges/ID
Reference:	DODD 5230.20, Enclosure 4, para E4.2.2
Default Vulnerability Discussion:	Failure to properly identify foreign nationals could lead to the loss or compromise of classified or sensitive information.
Default Finding Details:	
Default Recommendation:	Ensure FLOs are required to wear their own countys uniform with a badge identifying them as foreign nationals.
Supplemental Information:	SIPRNet Compliance Validation

Screen Sort Order:	FN - 040	**Report Sort Order:**	FN - 040	**PDI Key**	5458
Short Description Identifier:	FN - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	Foreign Liaison Officers (FLOs) are not prohibited from wearing nametags or using other titles that may be interpreted to infer or imply that they are U.S government personnel.				
Default Severity:	Category II			**Category:**	15E-Procedures
Reference:	DODD 5230.20, Enclosure 4, para E4.2.2				
Default Vulnerability Discussion:	Failure to properly identify foreign nationals could lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Ensure FLOs are not wearing nametags or using titles that may be interpreted to infer or imply that they are U.S government personnel.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	FN - 060	**Report Sort Order:**	FN - 060	**PDI Key**	5460
Short Description Identifier:	FN - 060			**Process Status:**	Production
External System ID:					
PDI Short Description:	A contact officer has not been appointed to control the activities of foreign visitors, FLO, and exchange personnel.				
Default Severity:	Category III			**Category:**	15E-Procedures
Reference:	DOD 5230.20, para 4.9				
Default Vulnerability Discussion:	Failure to limit access to Foreign Nationals to classified information can result in the loss or compromise of NOFORN information.				
Default Finding Details:					
Default Recommendation:	Appoint a Contact Officer to control the activities of all foreign personnel.				

Supplemental Information:	SIPRNet Compliance Validation

Screen Sort Order:	ID - 010	**Report Sort Order:**	ID - 010	**PDI Key**	5461
Short Description Identifier:	ID - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	A copy of the DD Form 254 is not on file for all contracts in which contractors have access to classified.				
Default Severity:	Category II			**Category:**	19G-Industrial Security Program
Reference:	DOD 5220.22-R, Appendix D				
Default Vulnerability Discussion:	Failure to complete a DD Form 254 or to specify security clearance and/or ADP requirements for all contracts that require access to classified material can result in unauthorized personnel having access to classified material or mission failure if personnel are not authorized the proper access.				
Default Finding Details:					
Default Recommendation:	DD Form 254s should be maintained on file for all classified contracts to ensure that all security requirements are being met.				
Supplemental Information:					

Screen Sort Order:	ID - 030	**Report Sort Order:**	ID - 030	**PDI Key**	5463
Short Description Identifier:	ID - 030			**Process Status:**	Production
External System ID:					
PDI Short Description:	The organization does not require contractors to submit Visit Authorization Letters (VALs) when visiting government facilities or the VAL does not contain all required information.				
Default Severity:	Category III			**Category:**	19G-Industrial Security Program
Reference:	DOD 5220.22-M, para 6-103 and para 6-104				
Default Vulnerability Discussion:	Failure to require VALs for contractor visits could result in sensitive or classified materials being released to unauthorized personnel.				
Default Finding Details:					
Default Recommendation:	Ensure all government facilities have a VAL on file for all contractors visiting the site.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 010	**Report Sort Order:**	IS - 010	**PDI Key**	5464
Short Description Identifier:	IS - 010			**Process Status:**	Production
External System ID:					

PDI Short Description:	Procedures have not been established to ensure safes, vaults, and secure rooms are properly managed and/or these procedures are not being adhered to.		
Default Severity:	Category II	**Category:**	10F-Storage
Reference:	DOD 5200.1-R, Chapter 6		
Default Vulnerability Discussion:	Improper procedures could result in the loss or compromise of classified material.		
Default Finding Details:			
Default Recommendation:	Establish a program to ensure safes, vaults, and secure rooms are properly managed. a. Ensure only GSA approved security containers are being utilized. Section 4, para 6-401 b. Ensure combinations are changed as required. Section 4, para 6-404b c. Ensure all forms; SF 700 and SF 702, are properly completed. Section 4, para 6-404b(3) and Section 3, para 6-302 d. Ensure repairs are conducted correctly. Section 4, para 6-405		
Supplemental Information:	SIPRNet Compliance Validation		

Screen Sort Order:	IS - 020	**Report Sort Order:**	IS - 020	**PDI Key**	5465
Short Description Identifier:	IS - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	The vaults and/or secure rooms for storage of classified material do not meet the physical security standards of DOD 5200.1-R, Appendix G.				
Default Severity:	Category I			**Category:**	10F-Storage
Reference:	DOD 5200.1-R, Appendix G				
Default Vulnerability Discussion:	Failure to meet standards could result in the loss or compromise of classified material.				
Default Finding Details:					
Default Recommendation:	Ensure vaults and secure rooms meet all requirements of Appendix G as follows: a. Vault standards - Section A, para 1. b. Secure room standards - Section A, para 2 c. Intrusion Detection System (IDS) Standards - Section B d. Access Controls - Section D				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 030	**Report Sort Order:**	IS - 030	**PDI Key**	5466
Short Description Identifier:	IS - 030			**Process Status:**	Production
External System ID:					
PDI Short Description:	Intrusion Detection System (IDS) monitoring stations are not being monitored by US citizens who have been subjected to a trustworthiness determination in accordance with DOD 5200.2-R.				
Default Severity:	Category II			**Category:**	15D-Intrusion Detection
Reference:	DOD 5200.1-R, appendix G para 6b				

Default Vulnerability Discussion:	Failure to subject personnel who monitor the IDS alarms to a trustworthiness determination can result in the inadvertent or deliberate release of classified material.
Default Finding Details:	
Default Recommendation:	Require the current IDS monitors be the subjects of a trustworthiness determination in accordance with DOD 5200.2-R or transfer the responsibility to a station manned by personnel who meet this requirement.
Supplemental Information:	SIPRNet Compliance Validation

Screen Sort Order:	IS - 040	**Report Sort Order:**	IS - 040	**PDI Key**	5467
Short Description Identifier:	IS - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	Classified documents, media, or equipment are not properly marked with the highest classification of the material/processing and any additional markings/designations as required.				
Default Severity:	Category II			**Category:**	10C-Classification Marking
Reference:	DOD 5200.1-R, Chapter 5; DOD 5200.1-PH; CJCSI 6510.01C, Enclosure B, para 1o(5)(b)				
Default Vulnerability Discussion:	Failure to properly mark classified material could result in the loss or compromise of classified information.				
Default Finding Details:					
Default Recommendation:	Properly mark all classified material, to include documents, media, and equipment. Electronic labeling, designation or marking shall clearly identify all classified material. If physical marking of the medium containing classified information is not possible, then identification of classified information must be accomplished by other means.				
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification				

Screen Sort Order:	IS - 050	**Report Sort Order:**	IS - 050	**PDI Key**	5468
Short Description Identifier:	IS - 050			**Process Status:**	Production
External System ID:					
PDI Short Description:	Classified material and equipment are not stored in accordance with its highest classification level or to the level of classified data being processed.				
Default Severity:	Category I			**Category:**	10F-Storage
Reference:	DOD 5200.1-R, para 6-402				
Default Vulnerability Discussion:	Failure to store classified in an approved container can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	If classified material is to be stored or processed, establish a secure means of storing all classified material. Approved storage may be in a GSA approved safe, vault, or an approved secure room. Ensure storage meets or exceeds requirements for the classification level and type of material stored.				
Supplemental	SIPRNet Compliance Validation				

Information:

Screen Sort Order:	IS - 060	**Report Sort Order:**	IS - 060	**PDI Key**	5469
Short Description Identifier:	IS - 060			**Process Status:**	Production
External System ID:					
PDI Short Description:	Personnel who are granted access to classified information do not have a valid Need-to-Know, proper security clearance, and/or have not executed a Non-Disclosure Agreement.				
Default Severity:	Category I			**Category:**	10-INFOSEC
Reference:	DOD 5200.1-R, para 1-101e, para 6-200 and para 9-200b				
Default Vulnerability Discussion:	Failure to verify clearance, need-to-know, and execute a non-disclosure agreement before granting access to classified can result in unauthorized personnel having access to classified.				
Default Finding Details:					
Default Recommendation:	Prior to receiving access to classified information it must be determined that an individual has met the following requirements: a. The person has the appropriate clearance and access eligibility. b. The person has signed an approved non-disclosure agreement. c. The person has a need-to-know the information.				
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification				

Screen Sort Order:	IS - 070	**Report Sort Order:**	IS - 070	**PDI Key**	5470
Short Description Identifier:	IS - 070			**Process Status:**	Production
External System ID:					
PDI Short Description:	Classified materials are not properly handled when removed from authorized storage.				
Default Severity:	Category I			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, para 6-301				
Default Vulnerability Discussion:	Failure to protect classified when removed from storage can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	SOP must describe the proper care of classified material when removed from approved storage. All employees granted access to classified must be briefed on proper handling procedures, to include the use of cover sheets and for maintaining positive control of the material.				
Supplemental Information:					

Screen Sort Order:	IS - 080	**Report Sort Order:**	IS - 080	**PDI Key**	5471
Short Description Identifier:	IS - 080			**Process Status:**	Production
External System ID:					

PDI Short Description:	Classified monitors/displays are not adequately safeguarded from viewing by unauthorized personnel to include foreign nationals.		
Default Severity:	Category I	**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, DODD 5230.20, para 4.7 and para 4.14 and CJCSI 6211.02A, Enclosure A, para 7a		
Default Vulnerability Discussion:	Failure to limit access to unauthorized personnel to classified information can result in the loss or compromise of classified information, including NOFORN information.		
Default Finding Details:			
Default Recommendation:	1. Position monitors so that they are not easily viewed by unauthorized persons and are under US personnel control at all times. 2. Follow escort procedures of announcing unauthorized personnel in the area. 3. Ensure that Foreign Nationals are escorted when they are in the immediate vicinity of US classified workstations and components.		
Supplemental Information:	SIPRNet Compliance Validation		

Screen Sort Order:	IS - 090	**Report Sort Order:**	IS - 090	**PDI Key**	5472
Short Description Identifier:	IS - 090			**Process Status:**	Production
External System ID:					
PDI Short Description:	Procedures have not been established for End-of-Day checks and/or the checks are not being accomplished for activities/facilities that process, handle and/or store classified material.				
Default Severity:	Category II			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, para 6-302				
Default Vulnerability Discussion:	Failure to have written guidance can result in end-of-day checks not being properly conducted and can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Ensure end-of-day checks are accomplished and as a minimum the following areas are checked: a. All vaults, secure rooms and containers used for the storage of classified material are properly secured. b. All classified material has been properly stored. c. All windows and doors are properly secured. d. Additional checks such as turning off of coffee pots, securing of STU III keys, etc can be identified and accomplished as part of the check. e. The SF 701, Activity Security Checklist shall be used to record these checks, to include after hours, weekend and holiday activities.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 100	**Report Sort Order:**	IS - 100	**PDI Key**	5473
Short Description Identifier:	IS - 100			**Process Status:**	Production

External System ID:					
PDI Short Description:	Proper procedures are not being followed when reproducing classified material.				
Default Severity:	Category III			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, Chapter 6, Section 5				
Default Vulnerability Discussion:	Improper reproduction procedures of classified material could result in the loss or compromise of classified information.				
Default Finding Details:					
Default Recommendation:	Ensure proper procedures are established and documented for reproducing classified material.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 110	**Report Sort Order:**	IS - 110	**PDI Key**	5474
Short Description Identifier:	IS - 110			**Process Status:**	Production
External System ID:					
PDI Short Description:	Classified material is not properly wrapped in preparation for transmission or it not being properly transmitted.				
Default Severity:	Category I			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, Chapter 7, Sections 1 and 2				
Default Vulnerability Discussion:	Failure to properly wrap and transmit classified material can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Develop an SOP on the proper method of wrapping classified to be shipped via an authorized method. Ensure appropriate wrapping materials are available. Train all applicable personnel on wrapping and shipping of classified.				
Supplemental Information:					

Screen Sort Order:	IS - 120	**Report Sort Order:**	IS - 120	**PDI Key**	5475
Short Description Identifier:	IS - 120			**Process Status:**	Production
External System ID:					
PDI Short Description:	Written authorization and briefings are not provided to persons who escort or carry classified materials off the installation and/or aboard commercial aircraft (domestic and international).				
Default Severity:	Category II			**Category:**	13F-Workforce Security Training
Reference:	DOD 5200.1-R, Chapter 7, Section 3				
Default Vulnerability Discussion:	Failure to provide couriers with the proper written authorization and training can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					

Default Recommendation:	Ensure all personnel are briefed that the hand-carrying or escorting of classified material requires a courier card or courier order. SOP must include procedures for requesting courier authorization, training of couriers, and maintaining records of training and courier authorization.
Supplemental Information:	

Screen Sort Order:	IS - 130	**Report Sort Order:**	IS - 130	**PDI Key**	5476
Short Description Identifier:	IS - 130			**Process Status:**	Production
External System ID:					
PDI Short Description:	Classified working papers are not properly marked, destroyed when no longer needed, or treated as a finished document after 180 days.				
Default Severity:	Category III			**Category:**	10E-Procedures
Reference:	DoD 5200.1-R, para 6-101				
Default Vulnerability Discussion:	Failure to properly mark or handle classified documents can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be: a. Dated when created; b. Marked with the highest classification of any information contained therein; c. Protected in accordance with the assigned classification; d. Conspicuously marked Working Paper on the first page of the document in letters larger than the text. e. Destroyed when no longer needed; and f. Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when retained more than 180 days from date of origin or released by the originator outside the activity.				
Supplemental Information:					

Screen Sort Order:	IS - 140	**Report Sort Order:**	IS - 140	**PDI Key**	5552
Short Description Identifier:	IS - 140			**Process Status:**	Production
External System ID:					
PDI Short Description:	Classified material is not being destroyed in an approved method for level of classification or type of material.				
Default Severity:	Category II			**Category:**	10E-Procedures
Reference:	DoD 5200.1-R, para 6-701				
Default Vulnerability Discussion:	Failure to properly destroy classified material can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Establish procedures for the destruction of classified material using approved methods based on the type of material to be destroyed. a. Methods and equipment used to routinely destroy paper classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing.				

	b. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification

---

Screen Sort Order:	IS - 150	**Report Sort Order:**	IS - 150	**PDI Key**	5477
Short Description Identifier:	IS - 150			**Process Status:**	Production
External System ID:					
PDI Short Description:	Plans have not been developed for the protection, removal, or destruction of classified material in case of emergency.				
Default Severity:	Category II			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, para 6-303				
Default Vulnerability Discussion:	Failure to develop emergency procedures can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	a. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. The level of detail and amount of testing and rehearsal of these plans should be determined by an assessment of the risk of hostile action, natural disaster, or terrorist activity that might place the information in jeopardy. b. These emergency planning procedures do not apply to material related to COMSEC. Planning for the emergency protection including emergency destruction under no-notice conditions of classified COMSEC material shall be developed IAW requirements of National Telecommunications Information Systems Security Instruction (NTSSI) 4004. c. When preparing emergency plans, consideration should be given to: 1. Reduction of the amount of classified material on hand 2. Storage of less frequently used classified material at more secure locations 3. Transfer of as much retained classified information to microforms or to removable automated information systems media as possible, thereby reducing its bulk. 4. Plans must include destruction of classified systems, media, and other forms, as well as paper.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 160	**Report Sort Order:**	IS - 160	**PDI Key**	5478
Short Description Identifier:	IS - 160			**Process Status:**	Production
External System ID:					
PDI Short Description:	The security manager does not conduct annual security self-inspections and ensure discrepancies are corrected.				
Default Severity:	Category II			**Category:**	10-INFOSEC
Reference:	E.O. 12958, Section 5.1; DOD 5200.1-R, para 1-700				

Default Vulnerability Discussion:	Failure to conduct self-inspections results in a weak security program and can lead to the loss or compromise of classified or sensitive information.
Default Finding Details:	
Default Recommendation:	Appointed security managers will conduct annual self-inspections of their traditional security programs. Self-inspection should review the following areas as a minimum: a. Information Security b. Information System Security c. Personnel Security d. Physical Security
Supplemental Information:	

Screen Sort Order:	IS - 170	**Report Sort Order:**	IS - 170	**PDI Key**	5479
Short Description Identifier:	IS - 170			**Process Status:**	Production
External System ID:					
PDI Short Description:	Individuals assigned to the organization are not aware of their responsibilities in reporting possible security compromises.				
Default Severity:	Category II			**Category:**	10D-Incident Reporting
Reference:	DOD 5200.1-R, para 10-101				
Default Vulnerability Discussion:	Failure to report possible security compromise can result in the impact of the loss or compromise of classified information not to be evaluated nor blame affixed.				
Default Finding Details:					
Default Recommendation:	SOP should include identification and recommended actions in the event of a security violation. These procedures must be included in initial and periodic security training for all personnel.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 180	**Report Sort Order:**	IS - 180	**PDI Key**	5480
Short Description Identifier:	IS - 180			**Process Status:**	Production
External System ID:					
PDI Short Description:	The Original Classification Authority (OCA) has not been appointed in writing and/or is not receiving training, prior to appointment. The OCA has been appointed by name and not by position.				
Default Severity:	Category II			**Category:**	19A-Appointments
Reference:	DoD 5200.1-R, para 9-301				
Default Vulnerability Discussion:	Failure to properly appoint and train an OCA can result in the improper classification of material.				
Default Finding Details:					
Default Recommendation:	Ensure the OCA is appointed in writing by the proper authority and that the appointment is by position and not by name. Prior to appointment, ensure the OCA is trained on the responsibilities of an OCA.				
Supplemental					

Information:

Screen Sort Order:	IS - 190	**Report Sort Order:**	IS - 190	**PDI Key**	5481
Short Description Identifier:	IS - 190			**Process Status:**	Production
External System ID:					
PDI Short Description:	Offices do not have classification guides available which are applicable to their operations.				
Default Severity:	Category II			**Category:**	19B-Procedures and Policies
Reference:	DOD 5200.1-R, para 2-502b				
Default Vulnerability Discussion:	Failure to have proper classification guidance can result in the misclassification of information and can lead to the loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Security classification guides shall be distributed by the originating organization to those organizations and activities they believe will be derivatively classifying information covered by the guide. Obtain any required classification guides not on hand.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	IS - 200	**Report Sort Order:**	IS - 200	**PDI Key**	5482
Short Description Identifier:	IS - 200			**Process Status:**	Production
External System ID:					
PDI Short Description:	Controlled Unclassified Information is not handled, marked, stored, transmitted, or destroyed in an approved manner.				
Default Severity:	Category III			**Category:**	10G-Unclassified Controlled Information
Reference:	DOD 5200.1-R, Appendix C				
Default Vulnerability Discussion:	Failure to handle CUI in an approved manner can result in the loss or compromise of sensitive information.				
Default Finding Details:					
Default Recommendation:	Develop a program to properly handle Controlled Unclassified Information (CUI). CUI includes For Official Use Only information, Sensitive But Unclassified (formerly Limited Official Use) information, DEA Sensitive Information, DoD Unclassified Controlled Nuclear Information, Sensitive Information as defined in the Computer Security Act of 1987, and information contained in technical documents. SOPs should define Controlled Unclassified Information and identify proper marking, storing, transmission, destruction, and release.				
Supplemental Information:					

Screen Sort Order:	IS - 230	**Report Sort Order:**	IS - 230	**PDI Key**	5485
Short Description Identifier:	IS - 230			**Process Status:**	Production
External System ID:					
PDI Short Description:	The annual review and clean out day for classified material was not conducted.				
Default Severity:	Category III			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, para 6-700b and DISAI 240-110-8, para 9-4, para 13-5e(8)				
Default Vulnerability Discussion:	Failure to conduct the annual review and clean out day can result in an excessive amount of classified being on hand and therefore being harder to account for, resulting in the possibility of loss or compromise of classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Conduct the annual review and clean out day, and maintain a record of the results under normal file management regulations.				
Supplemental Information:					

Screen Sort Order:	IS - 260	**Report Sort Order:**	IS - 260	**PDI Key**	8937
Short Description Identifier:	IS - 260			**Process Status:**	Production
External System ID:					
PDI Short Description:	Procedures have not been established when classified meetings or conferences are to be held.				
Default Severity:	Category I			**Category:**	10E-Procedures
Reference:	DOD 5200.1-R, para 6-307				
Default Vulnerability Discussion:	Unauthorized personnel could obtain classified information resulting is an loss/compromise of classified information.				
Default Finding Details:					
Default Recommendation:	Establish written procedures for holding classified meetings/conferences.				
Supplemental Information:					

Screen Sort Order:	ISS - 010	**Report Sort Order:**	ISS - 010	**PDI Key**	5363
Short Description Identifier:	ISS - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	Adequate fire detection and suppression does not exist or is not periodically tested.				
Default Severity:	Category III			**Category:**	17A1-Detection
Reference:	FIPS PUB 31, NFPA 75, and DODI 8500.2 Enclosure 4 Control Numbers PEFD-2, PEFI-1 and PEFS-2 located in Attachments 1, 2 and 3				
Default Vulnerability Discussion:	Failure to provide adequate fire detection and suppression could result in the loss of or damage to data, equipment, facilities, or personnel.				

Default Finding Details:

Default Recommendation:	Ensure adequate fire detection and suppression are available, commensurate with the size of the system. Fire detection and suppression must be periodically tested to ensure effectiveness.
Supplemental Information:	Ask if server room has sprinklers or a hand-held fire extinguisher within 50 feet of equipment. Visually inspect area. Ensure fire extinguisher is minimally rated for electrical fires (Class C in the form of carbon dioxide, dry chemical or halon type agents.

Screen Sort Order:	ISS - 020	**Report Sort Order:**	ISS - 020	**PDI Key**	5488
Short Description Identifier:	ISS - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	Security Features Users Guides or equivalent (such as Security Standard Operating Procedure) have not been developed or are not available for all systems in the organization.				
Default Severity:	Category III			**Category:**	19C2-SFUG
Reference:	CJCSI 6510.01C Enclosure B para 1o(31)(c) and para 1o(43), DODI 8500.2 para 5.10.5 and DODI 8500.2 Enclosure 4 Control Number PRRB-1 located in Attachments 1, 2 and 3				
Default Vulnerability Discussion:	If user guides are not available for the end users, the security features of the systems are weakened and can possibly result in easy compromise by hackers or unauthorized individuals.				
Default Finding Details:					
Default Recommendation:	Ensure user guides are available for all systems and as a minimum the following areas are documented: a. Handling of suspected system compromise b. Information Operations Condition (INFOCON) procedures and policies c. Periods Processing (if applicable) d. Procedures for eradication after an attack e. Proper password management f. Purging of storage media (disks, drives, etc) prior to turn-in or disposal g. Remote diagnostic and maintenance h. Turn-in of equipment i. Use of screensavers/Unattended terminals j. Virus detection and scanning k. Warning Banners				
Supplemental Information:	Ask if an SFUG or Security SOP has been developed and approved. View copy if time permits to ensure required topics are covered.				

Screen Sort Order:	ISS - 030	**Report Sort Order:**	ISS - 030	**PDI Key**	5489
Short Description Identifier:	ISS - 030			**Process Status:**	Production
External System ID:					
PDI Short Description:	There is no configuration management process (which includes the IAO/IAM) to evaluate and approve system changes to software, firmware, and hardware that will affect the security of the system.				
Default Severity:	Category II			**Category:**	14-Configuration Management
Reference:	NIST 800-14, para 3.9, DODD 8500.1 para 4.17; DODI 8500.2 Enclosure 4 Control Number DCPR-1 located in attchments 1, 2 and 3; DODI 8500.2				

	Enclosure 4 Control Number DCCB-1 located in attchments 1, 2 and 3
Default Vulnerability Discussion:	Security vulnerabilities may be introduced when changes take place in the environment that have not been reviewed by the security personnel in conjunction with a configuration control board process.
Default Finding Details:	
Default Recommendation:	The IAO/IAM is responsible for ensuring that there are no security risks presented by software, firmware, or hardware introduced at the facility. Implement a configuration management process that includes the IAO/IAM.
Supplemental Information:	Ask the IAM if a configuration control board (CCB) exists and if security is a participating member of the CCB. If time permits ask to see a copy of the CCB charter or other documentation.

Screen Sort Order:	ISS - 040	**Report Sort Order:**	ISS - 040	**PDI Key**	5490
Short Description Identifier:	ISS - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	Continuity of Operations Plans (COOP) have not been developed and/or tested to ensure system and data availability in the event of any type of failure. COOP is not commensurate with the assigned Mission Assurance Category (MAC) for the system(s).				
Default Severity:	Category II			**Category:**	21C-COOP/DRP
Reference:	CJCSI 6510.01C Enclosure B para 1o(39); DODD 8500.1, para 4.7; DODI 8500.2 IA Controls CODP-1, CODP-2 CODP-3; OMB Circular NO. A-130, Appendix III, para A3a2e				
Default Vulnerability Discussion:	Failure to develop a COOP and test it periodically can result in the partial or total loss of operations and INFOSEC. A contingency plan is necessary to reduce mission impact in the event of system compromise or disaster.				
Default Finding Details:					
Default Recommendation:	COOP/Disaster Recovery/Contingency plan should address the following: a. The system has a tested contingency plan addressing full system restoration. b. Identify the use of another system to be used to avoid interruption of important processing, if the system were destroyed, or in need of repair. c. Backups are made of critical applications on a regular basis, are selectively tested on a regular basis, and are stored off-site, and the security posture of the off-site location is adequate for their storage. d. A current, tested, system Emergency Action Plan exists, and assigns clear responsibilities for actions to be taken during the emergency situation. These actions are listed in priority order. The Emergency Action plan is tested periodically to test events with less than catastrophic occurrences as well as events with major catastrophic occurrences. e. A system Backup Plan exists and: 1. Identifies critical and vital files, which must be backed up to include how the media containing those files are to be marked. 2. Identifies essential documentation that must be available in the event the primary processing site is unavailable. 3. Establishes the frequency of backups and rotation schedule of the backup media. 4. Provides for off site storage of the backed up media and essential documentation. 5. Contains information relating to security of the backed up media, to include while being transported to/from the off-site location. 6. Contains information regarding a backup computer facility. f. A Disaster Recovery Plan exists and: 1. Establishes evaluation criteria for determining the extent of disruption of functions and operations.				

	2. Identifies backup processing site(s). 3. Covers the safeguarding or destruction of classified or sensitive information in the event that the primary site must be evacuated. 4. Provides detailed plans for the movement of personnel and the backup media/documentation to the backup processing site. 5. Provides guidance for testing the plan. g. Responsibilities are clearly and unambiguously assigned in the Contingency Plan. h. The organizations Contingency Plans clearly outlines the amount of downtime that can be tolerated before disaster is declared. i. The comprehensiveness of the COOP is dependant upon the MAC Level of the system or enclave, MAC I being the highest criticallity.
Supplemental Information:	Ask if COOP plan has been: developed, documented, approved, and tested. Was COOP developed commensurate with the assigned MAC Level.

Screen Sort Order:	ISS - 050	**Report Sort Order:**	ISS - 050	**PDI Key**	5491
Short Description Identifier:	ISS - 050			**Process Status:**	Production
External System ID:					
PDI Short Description:	A program does not exist to recognize, investigate, and report information systems security incidents to include virus, system penetration, and classified contamination.				
Default Severity:	Category II			**Category:**	22B1-Incident Actions
Reference:	CJCSI 6510.01C, Enclosure A, para 2z(2)(c); CJCSI 6510.01C Enclosure B, para 1a(4)(c); DODI 8500.2 para 5.8.5, para 5.9.10 and para 5.12.3				
Default Vulnerability Discussion:	Failure to recognize, investigate and report information systems security incidents could result in the loss of confidentiality, integrity, and availability of the systems and its data.				
Default Finding Details:					
Default Recommendation:	Establish a program to recognize, investigate, and report information systems security incidents.				
Supplemental Information:	Ask to see computer security incident handling procedures either in a Security SOP or other document. Review if time permits to ensure completeness.				

Screen Sort Order:	ISS - 060	**Report Sort Order:**	ISS - 060	**PDI Key**	5492
Short Description Identifier:	ISS - 060			**Process Status:**	Production
External System ID:					
PDI Short Description:	Memorandums of Agreements (MOAs) or Memorandums of Understanding (MOUs) are not available when the system is connected to other networks under authority of another DAA.				
Default Severity:	Category II			**Category:**	11A4-SLA/MOA with Customers
Reference:	CJCSI 6510.01C Enclosure B para 1o(11); DODI 8500.2 Enclosure 4 Control Number DCID-1 located in Attachments 1, 2 and 3				
Default Vulnerability Discussion:	Failure to have MOAs/MOUs in place can result in a vulnerability to the system and network.				
Default Finding Details:					
Default	Ensure MOAs or MOUs are available when the system is connected to other				

Recommendation:	networks under authority of another DAA.
Supplemental Information:	Ask if there are any connections to another enclave, under the control of different DAA. If so, ask if an MOU is in place. If possible review network diagrams to confirm or deny existence of interconnections and ask to see MOU. MOU should be signed by both organizations.

Screen Sort Order:	ISS - 090	**Report Sort Order:**	ISS - 090	**PDI Key**	5495
Short Description Identifier:	ISS - 090			**Process Status:**	Production
External System ID:					
PDI Short Description:	A System Access Control Form (DD Form 2875 or equivalent) is not being used to define and control individual access.				
Default Severity:	Category II			**Category:**	11-User-ID Administration
Reference:	DODI 8500.2 Enclosure 4 Attachment 4 Control Number IAAC-1; DODI 8500.2 para 5.10.1 and para 5.11.2; CJCSM 6510.01 Appendix A Enclosure A para 8 (draft)				
Default Vulnerability Discussion:	If accurate records of authorized users are not maintained, then unauthorized personnel could have access to the system.				
Default Finding Details:					
Default Recommendation:	Initiate a System Access Control Form for each person who requests logon access to a computer system. The IAO will retain all forms for each person granted access to their systems.				
Supplemental Information:	Ask to review the user registration form being used to document users. If not a DD Form 2875, ensure their form has the same functionality.				

Screen Sort Order:	ISS - 100	**Report Sort Order:**	ISS - 100	**PDI Key**	5494
Short Description Identifier:	ISS - 100			**Process Status:**	Production
External System ID:					
PDI Short Description:	There is no procedure that implements DOD policy to ensure that users, System Administrators and Network Administrators are properly trained and certified.				
Default Severity:	Category II			**Category:**	13-Training
Reference:	CJCSI 6510.01C, Enclosure A, para 2T(1)				
Default Vulnerability Discussion:	Improperly trained personnel can cause serious system-wide/network-wide problems that render a system/network unstable.				
Default Finding Details:					
Default Recommendation:	Develop a procedure to ensure that all DOD personnel and support contractors are trained and appropriately certified to perform the tasks associated with their responsibilities for safeguarding and operating DOD information systems.				
Supplemental Information:	Ask if System Administrators are at least Level 1 certified. Is the policy requiring certification contained in their Security SOP? Do all users receive initial IA training before being given access to the system?				

Screen Sort Order:	ISS - 110	**Report Sort Order:**	ISS - 110	**PDI Key**	5497

Short Description Identifier:	ISS - 110	**Process Status:**	Production
External System ID:			
PDI Short Description:	There is not a least privilege policy in effect that ensures the user has access to all of the information to which the user is entitled, but to no more, to include foreign nationals if they are approved for access.		
Default Severity:	Category II	**Category:**	12A-Access Controls
Reference:	DODI 8500.2 Enclosure 4 Control Number ECLP-1 located in Attachments 4, 5 and 6		
Default Vulnerability Discussion:	Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system.		
Default Finding Details:			
Default Recommendation:	Establish a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.		
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification		

Screen Sort Order:	ISS - 180	**Report Sort Order:**	ISS - 180	**PDI Key**	5504
Short Description Identifier:	ISS - 180			**Process Status:**	Production
External System ID:					
PDI Short Description:	A System Security Authorization Agreement (SSAA) and related security documents have not been developed and submitted to the appropriate authority for approval.				
Default Severity:	Category III			**Category:**	19C5-Technical Documentation
Reference:	DOD 8510.1-M, para C2.1.1.5				
Default Vulnerability Discussion:	Failure to provide the proper documentation can lead to a system connecting without all proper safeguards in place, creating a threat to the networks.				
Default Finding Details:					
Default Recommendation:	Ensure the SSAA and related security documentation are developed in accordance with DITSCAP requirements, properly submitted and approved. A copy of the SSAA and security documentation will be maintained on-site by the organization.				
Supplemental Information:	Ask to see a copy of the ATO/IATO letter. Is it current? Ask if a full SSAA support the ATO/IATO.				

Screen Sort Order:	ISS - 190	**Report Sort Order:**	ISS - 190	**PDI Key**	5505
Short Description Identifier:	ISS - 190			**Process Status:**	Production
External System ID:					
PDI Short Description:	Procedures are not developed to maintain the accredited baseline including notification to the approving authority in the event of changes to the baseline.				
Default Severity:	Category III			**Category:**	19C5-Technical Documentation
Reference:	CJCSI 6510.01, Appendix A to Enclosure A, para 1 (draft)				

Default Vulnerability Discussion:	Without proper procedures in place for maintaining the accredited baseline, changes could be made which would negate the accreditation of the system and possibly cause a disruption in the systems operation.
Default Finding Details:	
Default Recommendation:	Establish and maintain a set of procedures to properly maintain the accredited baseline of the system.
Supplemental Information:	Level 1 Certification

Screen Sort Order:	ISS - 200	**Report Sort Order:**	ISS - 200	**PDI Key**	5506
Short Description Identifier:	ISS - 200			**Process Status:**	Production
External System ID:					
PDI Short Description:	The command does not have at least an Interim Approval to Connect (IATC) to NIPRNET and must be in compliance with the NIPRNET Connection Approval Process to include a waiver for Internet connectivity, if applicable.				
Default Severity:	Category III			**Category:**	19C5-Technical Documentation
Reference:	CJCSI 6211.02B, Appexdix B to Encl C				
Default Vulnerability Discussion:	Failure to provide to the current connection documentation can result in a threat to the NIPRNet connected systems.				
Default Finding Details:					
Default Recommendation:	Ensure an IATC is obtained for connection to the NIPRNet by the organization.				
Supplemental Information:	ATC/IATC may be reviewed ahead of time on the NIPRNET database http://www.nic.mil/dodnic.mil/index_no.html or https://cap.nipr.mil. If not, ask to see at site. Ensure ATC/IATC is current. Check with technical reviewers to ensure there are no back-door connection to the Internet, that are not already covered by a waiver.				

Screen Sort Order:	ISS - 210	**Report Sort Order:**	ISS - 210	**PDI Key**	5507
Short Description Identifier:	ISS - 210			**Process Status:**	Production
External System ID:					
PDI Short Description:	The command does not have at least an Interim Approval to Connect (IATC) to SIPRNet from the SIPRNet Connection Approval Office (SCAO), an updated SIPRNet Access Assessment Form, and connection documentation in order for the SIPRNet to maintain the current level of certification. Copies of this documentation must be maintained and available on site.				
Default Severity:	Category III			**Category:**	19C5-Technical Documentation
Reference:	DISN Connection Security Requirements				
Default Vulnerability Discussion:	Failure to provide to the SCAO current connection documentation can result in a threat to the SIPRNet connected systems.				
Default Finding Details:					
Default Recommendation:	Provide the SCAO current certification documentation in accordance with the referenced message. In addition the site also has the responsibility to notify the SCAO of any changes to the approved architecture.				
Supplemental	SIPRNet Compliance Validation				

Information:

Screen Sort Order:	ISS - 220	**Report Sort Order:**	ISS - 220	**PDI Key**	5508
Short Description Identifier:	ISS - 220			**Process Status:**	Production
External System ID:					
PDI Short Description:	Approved switch boxes are not in use for switching between the different classification levels of SECRET and NON-SECRET information.				
Default Severity:	Category II			**Category:**	16N-Procedures
Reference:	DSAWG Meeting Minutes, paragraph F, 13 December 2000 and SIPRNet Connection Approval Office E-mail Message 26 April 2001				
Default Vulnerability Discussion:	Failure to use approved switch boxes can result in the loss or compromise of classified information.				
Default Finding Details:					
Default Recommendation:	Remove all unapproved switch boxes from the SIPRNet and install one of the approved switch boxes, or install separate keyboard, mouse and monitor for the workstations, or contact the SIPRNet Connection Approval Office (SCAO) for requesting approval of the unapproved switch box.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	ISS - 240	**Report Sort Order:**	ISS - 240	**PDI Key**	5510
Short Description Identifier:	ISS - 240			**Process Status:**	Production
External System ID:					
PDI Short Description:	Network connections (classified and unclassified) are not protected to the commensurate level of the information being process on the network.				
Default Severity:	Category I			**Category:**	15H-Computer Room/Server Protection
Reference:	CJCSI 6211.02A, para 7a				
Default Vulnerability Discussion:	Network connections that are not properly protected are highly vulnerable to unauthorized access, resulting in the loss or compromise of classified information.				
Default Finding Details:					
Default Recommendation:	Connected systems will be secured commensurate with the sensitivity of the information (both classified and unclassified) being processed. Modify the facility to meet storage standards or move equipment to another approve storage area.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	ISS - 290	**Report Sort Order:**	ISS - 290	**PDI Key**	5515
Short Description Identifier:	ISS - 290			**Process Status:**	Production
External System ID:					

PDI Short Description:	1. The command has not designated a primary and alternate point of contact responsible for Information Assurance Vulnerability Alert (IAVA). 2. The IAVA POC does not acknowledge receipt of all IAVA notifications within 5 days or report compliance via the appropriate IAVA web site, within 30 days.		
Default Severity:	Category II	**Category:**	10E-Procedures
Reference:	DEPSECDEF Memo, 30 Dec 99, para 2.a, b, d, 3.a		
Default Vulnerability Discussion:	The command will not be aware of the latest vulnerabilities and upgrades affecting their systems which could result in the loss or compromise of information.		
Default Finding Details:			
Default Recommendation:	Assign a primary and alternate POC, and ensure compliance in accordance with the DECSECDEF Memo.		
Supplemental Information:	Ask if the organization receives and applies IAVA notices. Is there an IAVA tracking system? VCTS is only required for DISA and other participating organizations.		

Screen Sort Order:	ISS - 330	**Report Sort Order:**	ISS - 330	**PDI Key**	5564
Short Description Identifier:	ISS - 330			**Process Status:**	Production
External System ID:					
PDI Short Description:	Procedures are not in place to identify access requests by foreign nationals.				
Default Severity:	Category II			**Category:**	10E-Procedures
Reference:	CJCSI 6510.01C, Enclosure A para 2n(2)(a)				
Default Vulnerability Discussion:	Unauthorized access by foreign nationals to Information Systems can result in, among other things, security incidents, compromise of the system, or the introduction of a virus.				
Default Finding Details:					
Default Recommendation:	Develop written procedures whereby all foreign access requests are documented and permitted only after a thorough review by security personnel.				
Supplemental Information:	Ask if any foreign nationals have access to the system. Ensure approval has been received to allow access. Access to NIPRNET requires service level approval.				

Screen Sort Order:	PE - 010	**Report Sort Order:**	PE - 010	**PDI Key**	5518
Short Description Identifier:	PE - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	Derogatory information is not referred to the commander or the security officer of the organization, to which the individual is assigned, in the most expeditious means possible. Derogatory information is not being submitted to the appropriate Consolidated Adjudicating Facility (CAF).				
Default Severity:	Category II			**Category:**	18D-Procedures
Reference:	DOD 5200.2-R, para 8-101a (Internet version para C8.1.2)				

Default Vulnerability Discussion:	Withholding derogatory information from the responsible adjudicative facility could result in an ineligible individual being granted access to classified or sensitive information.
Default Finding Details:	
Default Recommendation:	Develop a program/policy for reporting derogatory information and train all personnel on recognizing and reporting derogatory information.
Supplemental Information:	SIPRNet Compliance Validation

Screen Sort Order:	PE - 020	**Report Sort Order:**	PE - 020	**PDI Key**	5519
Short Description Identifier:	PE - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	Supervisory personnel are not familiar with their special responsibilities in matters pertaining to personnel security.				
Default Severity:	Category III			**Category:**	18D-Procedures
Reference:	DOD 5200.2-R, para 9-102 (Internet version para C9.1.3)				
Default Vulnerability Discussion:	Failure to advise supervisors of the personnel security responsibilities could lead to derogatory information not being reported and ineligible personnel having access to sensitive or classified information.				
Default Finding Details:					
Default Recommendation:	Security programs shall be established to insure that supervisory personnel are familiar with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	PE - 030	**Report Sort Order:**	PE - 030	**PDI Key**	5520
Short Description Identifier:	PE - 030			**Process Status:**	Production
External System ID:					
PDI Short Description:	Individuals are not familiar with pertinent security regulations nor are they aware of standards of conduct required of persons holding positions of trust.				
Default Severity:	Category III			**Category:**	18D-Procedures
Reference:	DOD 5200.2-R, para 9-103 (Internet version para C9.1.4)				
Default Vulnerability Discussion:	Failure to inform personnel of the expected standards of conduct while holding a position of trust can result in conduct by the individual that will require them being removed from that position.				
Default Finding Details:					
Default Recommendation:	Provide training to all employees on security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. Individuals must be able to recognize and avoid the kind of personal behavior that would result in rendering them ineligible for continued assignment in a position of trust.				
Supplemental	SIPRNet Compliance Validation				

Information:	Level 1 Certification

Screen Sort Order:	PE - 040	**Report Sort Order:**	PE - 040	**PDI Key**	5521
Short Description Identifier:	PE - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	DOD military, civilian and contractor positions (if required by DD Form 254) have not been designated with position sensitivity based on the required access of their position to classified information or other sensitive duties.				
Default Severity:	Category II			**Category:**	18D-Procedures
Reference:	DOD 5200.2-R para 3-101 or para 3-400 (Internet version para C3.1.2 or C3.4)				
Default Vulnerability Discussion:	Failure to designate position sensitivity could result in personnel having access to classified information or other sensitive duties without the required investigative and adjudicative prerequisites.				
Default Finding Details:					
Default Recommendation:	Ensure all DOD military, civilian and contractor positions are designated to reflect clearance requirements and any other sensitive duties. Review all positions for the correct clearance requirement.				
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification				

Screen Sort Order:	PE - 050	**Report Sort Order:**	PE - 050	**PDI Key**	5522
Short Description Identifier:	PE - 050			**Process Status:**	Production
External System ID:					
PDI Short Description:	Validation of security clearance has not been obtained for each individual given access to classified.				
Default Severity:	Category III			**Category:**	18B-Clearances
Reference:	DOD 5200.2-R, para 7-101 (Internet version para C7.1.1)				
Default Vulnerability Discussion:	Failure to verify security clearance status could result in an unauthorized person having access to classified information or an authorized person being unable to perform assigned duties.				
Default Finding Details:					
Default Recommendation:	Ensure a security clearance validation is obtained from an approved Personnel Security Roster or Clearance Certificate and posted to each individuals local security file.				
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification				

Screen Sort Order:	PE - 070	**Report Sort Order:**	PE - 070	**PDI Key**	5524
Short Description Identifier:	PE - 070			**Process Status:**	Production
External System ID:					

PDI Short Description:	DOD military, civilian personnel, and contractor personnel have not been assigned with one of the three IT (ADP) designations based on specific criteria as designated in DOD 5200.2-R, Appendix K (Internet version Appendix 10).		
Default Severity:	Category II	**Category:**	18C-ADP Sensitivity
Reference:	DOD 5200.2-R para 3-614 (Internet version para C3.6.15) and Appendix K (Internet version Appendix 10); DODD 8500.1, para 4.8 E2.1.24; CJCSI 6510.01C, Enclosure A, para 2n(5)		
Default Vulnerability Discussion:	Failure to designate an appropriate IT level could result in an individual having access to an information system without the required investigative and adjudicative prerequisites.		
Default Finding Details:			
Default Recommendation:	Ensure all positions; military, civilian, and contractors, are assigned to one of the three IT levels. Designations should be noted on Position Descriptions for Civilian Employees, JTD for Military Personnel, and in the Statement of Work or Contract for contractors.		
Supplemental Information:	Ask if an IT (ADP) Designation Program exists. Ask if all positions have been designated. Look at documentation such as DD Forms 2875 or Personnel Security Rosters to check if different IT levels are designated. Ask for proof of IT level of a known SA and confirm if IT I was granted and the individual has an SSBI (or it is in process.)		

Screen Sort Order:	PE - 080	**Report Sort Order:**	PE - 080	**PDI Key**	5525
Short Description Identifier:	PE - 080			**Process Status:**	Production
External System ID:					
PDI Short Description:	The correct investigation has not been submitted on all personnel; military, civilian and contractor, based upon their position sensitivity and IT level.				
Default Severity:	Category II			**Category:**	18A-Investigations
Reference:	DOD 5200.2-R, para 3-200 and para 3-400 (Internet version para C3.2 and C3.4)				
Default Vulnerability Discussion:	Failure to investigate personnel based upon their position sensitivity could result in unauthorized personnel having access to classified or sensitive information.				
Default Finding Details:					
Default Recommendation:	Ensure all personnel have the required investigation based upon their position sensitivity. Submit requests for investigation for personnel who have not had the correct investigation conducted. Implement a program to ensure personnel have the required investigations before the start of employment.				
Supplemental Information:					

Screen Sort Order:	PE - 090	**Report Sort Order:**	PE - 090	**PDI Key**	5526
Short Description Identifier:	PE - 090			**Process Status:**	Production
External System ID:					
PDI Short Description:	Periodic Reinvestigations are not submitted in the required time period as determined by the level of clearance and access.				

Default Severity:	Category III	**Category:**	18A-Investigations
Reference:	DOD 5200.2-R, para 3-700 (Internet version para C3.7)		
Default Vulnerability Discussion:	Failure to subject personnel to periodic reinvestigation can result in derogatory information not being discovered on personnel having access to sensitive or classified information.		
Default Finding Details:			
Default Recommendation:	Submit requests for Periodic Reinvestigation on all personnel to meet the 5-year requirement for SSBIs and 10-year requirement for NACLC or ANACI. Establish a program to keep all investigations current.		
Supplemental Information:			

Screen Sort Order:	PE - 100	**Report Sort Order:**	PE - 100	**PDI Key**	5527
Short Description Identifier:	PE - 100			**Process Status:**	Production
External System ID:					
PDI Short Description:	Waivers to investigative requirements are not approved at the appropriate level, prior to an individual being assigned to sensitive duties or having classified access.				
Default Severity:	Category III			**Category:**	18A-Investigations
Reference:	DOD 5200.2-R, para 3-800 (Internet version para C3.8)				
Default Vulnerability Discussion:	Failure to have waivers to investigative requirements approved before an individual is assigned to a sensitive position can lead to an unauthorized individual having access to sensitive or classified information.				
Default Finding Details:					
Default Recommendation:	Ensure all personnel have the required investigative requirement or an approved waiver before they are assigned to a sensitive position.				
Supplemental Information:					

Screen Sort Order:	PE - 110	**Report Sort Order:**	PE - 110	**PDI Key**	5528
Short Description Identifier:	PE - 110			**Process Status:**	Production
External System ID:					
PDI Short Description:	Non-U.S. citizens are assigned to sensitive duties or granted access to classified information without the appropriate Limited Access Authorization (LAA) granted.				
Default Severity:	Category I			**Category:**	18B-Clearances
Reference:	DOD 5200.2-R, para 2-100 and para 3-402 (Internet version para C2.1.1 and C3.4.3)				
Default Vulnerability Discussion:	Failure to verify citizenship could allow unauthorized personnel to have access to classified information.				
Default Finding Details:					
Default Recommendation:	Remove all non-U.S. citizens from their duty position and implement procedures to ensure all new personnel are screened for citizenship. If compelling reasons exist for the non-U.S. citizen to be assigned to sensitive				

	duties or have access to classified information, ensure the proper documentation is completed and/or a LAA is granted.
Supplemental Information:	SIPRNet Compliance Validation

Screen Sort Order:	PE - 120	**Report Sort Order:**	PE - 120	**PDI Key**	5529
Short Description Identifier:	PE - 120			**Process Status:**	Production
External System ID:					
PDI Short Description:	All contract guards are not subjects of a favorable NAC prior to assignment in a DOD facility.				
Default Severity:	Category III			**Category:**	18A-Investigations
Reference:	DOD 5200.2-R, para 3-612 (Internet version para C3.6.13)				
Default Vulnerability Discussion:	Failure to screen guards could result in employment of unsuitable personnel who are responsible for the safety and security of DOD personnel and facilities.				
Default Finding Details:					
Default Recommendation:	Ensure any person performing contract guard functions has been the subject of a favorably adjudicated NAC prior to such assignment. Ensure this requirement is part of any contract for guard services.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	PE - 130	**Report Sort Order:**	PE - 130	**PDI Key**	5530
Short Description Identifier:	PE - 130			**Process Status:**	Production
External System ID:					
PDI Short Description:	Foreign (local) nationals employed by DOD organizations overseas whose duties do not require access to classified information have not been the subject of a local records check as required by agreement with the host nation or Status of Forces Agreement (SOFA).				
Default Severity:	Category II			**Category:**	18-Personnel Security
Reference:	DOD 5200.2-R, para 3-608 (Internet version para C3.6.9)				
Default Vulnerability Discussion:	Failure to subject foreign nationals to background checks could result in the loss or compromise of classified or sensitive information by foreign sources.				
Default Finding Details:					
Default Recommendation:	Ensure all foreign (local) nationals employed by DOD organizations overseas are subject to the following record checks: a. Host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government. b. DCII c. FBI-HQ/ID (Where information exists regarding residence by the foreign national in the United States for one year or more since age 18).				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	PH - 010	**Report Sort Order:**	PH - 010	**PDI Key**	5533
Short Description Identifier:	PH - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	A physical security program has not been developed by the command establishing active and passive measures designed to prevent unauthorized access to installations, facilities, personnel, equipment, material, and documents that safeguard them from espionage, sabotage, damage and theft.				
Default Severity:	Category III			**Category:**	15E-Procedures
Reference:	DODD 5200-8R, Chapter 2, para C2.1.1				
Default Vulnerability Discussion:	Failure to have a physical security program could result in an increased risk to personnel, equipment, material and documents.				
Default Finding Details:					
Default Recommendation:	Develop a physical security program to provide guidance and the means to counter threats during peacetime, transition to war, and in wartime.				
Supplemental Information:	SIPRNet Compliance Validation Level 1 Certification				

Screen Sort Order:	PH - 020	**Report Sort Order:**	PH - 020	**PDI Key**	5534
Short Description Identifier:	PH - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	A risk analysis has not been conducted and documented for the systems and the facility.				
Default Severity:	Category III			**Category:**	19C3-Risk Analysis
Reference:	DOD 8510.1-M, para C2.2				
Default Vulnerability Discussion:	Failure to conduct a risk analysis could result in not implementing an effective countermeasure to a vulnerability or wasting resources on ineffective measures leading to a possible loss of classified, equipment, facilities, or personnel.				
Default Finding Details:					
Default Recommendation:	Prepare a risk analysis for the system and facility. The commander/director will sign the risk analysis, signifying acceptance of any residual risk.				
Supplemental Information:	Ask if a Risk Analysis has been conducted. It is normally documented in the SSAA. If time permits, ask to see/review it. The RA should be no older than the SSAA but is preferably updated annually.				

Screen Sort Order:	PH - 025	**Report Sort Order:**	PH - 025	**PDI Key**	8936
Short Description Identifier:	PH - 025			**Process Status:**	Production
External System ID:					
PDI Short Description:	Major components of sensitive systems, such as servers, hubs, and switches, allow physical access to personnel without the need-to-know.				
Default Severity:	Category II			**Category:**	15H-Computer

					Room/Server Protection
Reference:	DODI 8500.2, IA Control PECF-1				
Default Vulnerability Discussion:	Allowing access to systems processing sensitive information by personnel without the need-to-know could permit loss, destruction of data or equipment or a denial of service. Loss could be accidental damage or intentional theft or sabotage.				
Default Finding Details:					
Default Recommendation:	Ensure all major system assets such as servers, hubs, and switches are protected by at least a key locked room, separately zoned access control rooms, or locked computer cabinets.				
Supplemental Information:	Physically inspect room that houses the servers. For unclassified systems: is the room locked with a key, swipe card, or cipher lock? Can only the personnel who need access to the system have unescorted access? If the room is shared with other employees is the server located in a locked cabinet?				

Screen Sort Order:	PH - 030	**Report Sort Order:**	PH - 030	**PDI Key**	5535
Short Description Identifier:	PH - 030			**Process Status:**	Production
External System ID:					
PDI Short Description:	The areas housing the critical information technology systems are not designated as Restricted Areas.				
Default Severity:	Category II			**Category:**	15G-Restricted Areas
Reference:	DOD 5200.8-R, Chapter 6, para C6.2.4				
Default Vulnerability Discussion:	Failure to designate the areas housing the critical information technology systems as a restricted area may result in inadequate protection being assigned during emergency actions or the site having insufficient physical security protection measures in place.				
Default Finding Details:					
Default Recommendation:	Ensure the areas housing the critical information technology systems are designated as a restricted area and all required physical security measures are taken. This must be coordinated with installation security force.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	PH - 040	**Report Sort Order:**	PH - 040	**PDI Key**	5536
Short Description Identifier:	PH - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	Security in-depth is not used as layered and complimentary security controls to deter and detect unauthorized entry and movement within the facility, commensurate with the threat.				
Default Severity:	Category II			**Category:**	15E-Procedures
Reference:	DOD 5200.8-R, Chapter 2, para C2.1.4				
Default Vulnerability Discussion:	Failure to use security in-depth can result in a facility being over or under secured.				

Default Finding Details:	
Default Recommendation:	Ensure a security in-depth approach is used for facility security.
Supplemental Information:	

Screen Sort Order:	PH - 050	**Report Sort Order:**	PH - 050	**PDI Key**	5537
Short Description Identifier:	PH - 050			**Process Status:**	Production
External System ID:					
PDI Short Description:	A program has not been established to identify and control visitors in controlled areas.				
Default Severity:	Category II			**Category:**	15B-Facility Access System
Reference:	DODI 8500.2 Enclosure 4 Control Number PEVC-1 located in Attachments 4 and 5				
Default Vulnerability Discussion:	Failure to identify and control visitors could result in unauthorized personnel gaining access to the facility with the intent to compromise classified information, steal equipment, or damage equipment or the facility.				
Default Finding Details:					
Default Recommendation:	Establish a program to control visitors. Program will include verification of clearance/investigation status, personal identification of visitor, registering of visitors, proper badging, and escorts, if required.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	PH - 060	**Report Sort Order:**	PH - 060	**PDI Key**	5538
Short Description Identifier:	PH - 060			**Process Status:**	Production
External System ID:					
PDI Short Description:	Control of sensitive items is not maintained. This includes keys, badges, smart cards.				
Default Severity:	Category II			**Category:**	15E-Procedures
Reference:	DOD 5100.8-R, para C1.3.3 and Best Practices				
Default Vulnerability Discussion:	Lack of an adequate key/access device control could result in unauthorized personnel gaining access to the facility or systems with the intent to compromise classified information, steal equipment, or damage equipment or the facility.				
Default Finding Details:					
Default Recommendation:	Establish a control program for all sensitive items. Store master and extra keys or devices in a locked container, have all personnel sign for sensitive items and establish procedures to maintain logs.				
Supplemental Information:					

Screen Sort Order:	SM - 010	**Report Sort Order:**	SM - 010	**PDI Key**	5546

Short Description Identifier:	SM - 010	**Process Status:**	Production
External System ID:			
PDI Short Description:	1. A properly trained security staff, allowing for separation of duties with each individual assigned to specific duties, has not been appointed in writing. 2. Information Assurance Managers (IAMs) and Information Assurance Officers (IAOs) must be US citizens.		
Default Severity:	Category III	**Category:**	19A-Appointments
Reference:	DoD 5200.1-R, para 1-201c; DODI 8500.2 para 5.8.2 and 5.9.5; CJCSI 6510.01C, Enclosure B para 1t(8)		
Default Vulnerability Discussion:	Failure to appoint security personnel could result in a weak security program.		
Default Finding Details:			
Default Recommendation:	1. The position structure of the security staff should allow for separation of duties by filling the following positions as a minimum. a. An IAM is appointed to oversee the Information System Security Program. b. An IAO is appointed for each system or type of system in the organization. c. A Security Manager (SM) is appointed to oversee the Traditional Security Program. 2. All security professionals assigned to the security staff should have received the appropriate training. 3. All appointments should be in writing and signed by the current commander/director. 4. Ensure the IAM is a US citizen. 5. If IAO is newly appointed, they must be a US citizen. If the IAO was appointed prior to Feb 03 they must be under the supervision of an IAM who is a US citizen and be approved in writing by the DAA.		
Supplemental Information:	Ask for copies of the appointment order for the IAM, IAO, and if possible the SM. Ask if these employees have been trained and/or certified if applicable.		

Screen Sort Order:	SM - 020	**Report Sort Order:**	SM - 020	**PDI Key**	5547
Short Description Identifier:	SM - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	A program does not exist to ensure personnel out process through the security section.				
Default Severity:	Category III			**Category:**	18D-Procedures
Reference:	DOD 5200.1-R, para 9-500				
Default Vulnerability Discussion:	Failure to properly out process through the security section allows the possibility of unauthorized access to the facility and/or the systems.				
Default Finding Details:					
Default Recommendation:	Ensure that all personnel departing the organization out process through the security section, to include turning in of all access badges, classified or sensitive information and signing of SF 312 acknowledging debriefing.				
Supplemental Information:	Level 1 Certification				

Screen Sort Order:	SM - 030	**Report Sort Order:**	SM - 030	**PDI Key**	5548
Short Description	SM - 030			**Process Status:**	Production

Identifier:			
External System ID:			
PDI Short Description:	Standard Operating Procedures (SOPs) have not been developed detailing all security procedures that are specific to the organization.		
Default Severity:	Category III	**Category:**	19C4-Security SOP
Reference:	DoD 5200.1-R, para 1-202e and DoD 5220.22-R, para 1-107		
Default Vulnerability Discussion:	Failure to have documented procedures in an SOP could result in a security incident due to lack of knowledge by personnel assigned to the organization.		
Default Finding Details:			
Default Recommendation:	Develop a SOP that as a minimum covers the following items: a. Access Control b. Classified Handling c. Computer Security d. COTS Prohibition e. Data Sharing f. Derogatory Information Reporting g. Emergency Actions h. End Of Day Procedures i. Foreign National Access to AIS j. Foreign Travel k. Fraud Waste and Abuse l. Handling of incoming mail/packages m. Key Control n. Personnel Security o. Security Awareness training p. Security Incident and Reporting		
Supplemental Information:	SIPRNet Compliance Validation		

Screen Sort Order:	SM - 040	**Report Sort Order:**	SM - 040	**PDI Key**	5549
Short Description Identifier:	SM - 040			**Process Status:**	Production
External System ID:					
PDI Short Description:	Travel awareness briefings are not provided to personnel conducting foreign travel nor is a record being maintained of such travel.				
Default Severity:	Category III			**Category:**	13-Training
Reference:	DoDD 2000.12, para 5.9.5				
Default Vulnerability Discussion:	Failure of personnel to inform the security staff of foreign travel or of the security staff to provide travel awareness briefings could result in personnel being targeted for espionage, criminal or terrorist activities. This could lead to compromise of classified information or physical harm to personnel.				
Default Finding Details:					
Default Recommendation:	Establish a comprehensive travel awareness briefing to be presented to personnel as required prior to foreign travel.				
Supplemental Information:	SIPRNet Compliance Validation				

Screen Sort Order:	SM - 050	**Report Sort Order:**	SM - 050	**PDI Key**	5550
Short Description Identifier:	SM - 050			**Process Status:**	Production

External System ID:

PDI Short Description: Personnel do not receive initial indoctrination and annual training thereafter on the national security implications of their duties and individual responsibilities.

Default Severity: Category III **Category:** 13F-Workforce Security Training

Reference: DoDD 5200.1-R, para 9-600

Default Vulnerability Discussion: Failure to provide security training results in a weak security program and could lead to the loss or compromise of classified or sensitive information.

Default Finding Details:

Default Recommendation:
1. Provide initial training that covers all areas of security.
2. Establish an annual training plan that covers the following areas as a minimum:
a. Classified Handling
b. Communications Security
c. Computer Security
d. Counter-intelligence
e. Courier briefing (if applicable)
f. Reporting of derogatory information
g. Reporting of Security Incidents
h. Security of Laptop computers when traveling
i. Special access programs, NATO, COSMIC TS, etc (if applicable)
j. Use of personal computers for conducting official business
3. Ensure all training is documented and a copy is maintained to validate that the training has been conducted.

Supplemental Information: Ensure all uses receive initial IA training before being given an account on the system. Ask if annual/periodic refresher training is provided.

Screen Sort Order: SM - 060 **Report Sort Order:** SM - 060 **PDI Key** 5551

Short Description Identifier: SM - 060 **Process Status:** Production

External System ID:

PDI Short Description: The SM has not established a relationship with the local Counter-Intelligence Agency to be able to receive CI updates and warnings, and to report possible incidents in a timely manner.

Default Severity: Category III **Category:** 10D-Incident Reporting

Reference: DODI 5240.4

Default Vulnerability Discussion: Failure to establish a good working relationship with the local CI agency could result in not being informed of local threats and warnings leaving the organization vulnerable to the threat and/or a delay in reporting a possible incident.

Default Finding Details:

Default Recommendation: Establish a working relationship with the local CI agency to ensure information is shared and reported as needed. Request copies of all local threat assessments and warnings.

Supplemental Information: SIPRNet Compliance Validation

Screen Sort Order: SM - 070 **Report Sort Order:** SM - 070 **PDI Key** 5368

Short Description Identifier:	SM - 070	**Process Status:**	Production
External System ID:			
PDI Short Description:	Policies and procedures for the protection, use, and dissemination of Sensitive Compartmented Information (SCI) are not being properly followed.		
Default Severity:	Category II	**Category:**	19H-Sensitive Compartmented Information Program
Reference:	DOD 5105.21-M-1, para 5.5		
Default Vulnerability Discussion:	Failure to follow the policies and procedures could result in the inadvertent disclosure of SCI information.		
Default Finding Details:			
Default Recommendation:	Ensure policies and procedures are being adhered to for SCI.		
Supplemental Information:			

Screen Sort Order:	SM - 080	**Report Sort Order:**	SM - 080	**PDI Key**	5369
Short Description Identifier:	SM - 080			**Process Status:**	Production
External System ID:					
PDI Short Description:	Sensitive Compartmented Information (SCI) facilities are not approved/authorized by the proper authorities for storage and processing of SCI information.				
Default Severity:	Category II			**Category:**	19H-Sensitive Compartmented Information Program
Reference:	DCID 1/21				
Default Vulnerability Discussion:	Failure to store and process SCI in an properly approved/authorized facility could result in the inadvertent disclosure of SCI information.				
Default Finding Details:					
Default Recommendation:	Ensure SCI facilities are properly approved for storage and processing of SCI.				
Supplemental Information:					

Screen Sort Order:	TM - 010	**Report Sort Order:**	TM - 010	**PDI Key**	5543
Short Description Identifier:	TM - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	TEMPEST countermeasures were not considered prior to establishing a classified work area.				
Default Severity:	Category III			**Category:**	16P-Emanations
Reference:	DODD C-5200.19				
Default Vulnerability	Failure to implement required TEMPEST countermeasures could leave the				

Discussion:	system(s) vulnerable to a TEMPEST attack.
Default Finding Details:	
Default Recommendation:	Consider Tempest countermeasures prior to establishing a classified work area.
Supplemental Information:	Level 1 Certification

Screen Sort Order:	TM - 020	**Report Sort Order:**	TM - 020	**PDI Key**	5544
Short Description Identifier:	TM - 020			**Process Status:**	Production
External System ID:					
PDI Short Description:	A separation of at least 50 centimeters is not maintained between any RED processor and BLACK equipment, including administrative support equipment, located in DOD facilities outside the continental US.				
Default Severity:	Category II			**Category:**	16P-Emanations
Reference:	NSTISSAM TEMPEST 2/95A 3 Feb 2000				
Default Vulnerability Discussion:	Failure to maintain proper separation could result in emanations of classified information.				
Default Finding Details:					
Default Recommendation:	Ensure a minimum of 50 centimeters separates any RED processor from BLACK equipment.				
Supplemental Information:	Overseas Locations only SIPRNet Compliance Validation				

Screen Sort Order:	TM - 030	**Report Sort Order:**	TM - 030	**PDI Key**	5545
Short Description Identifier:	TM - 030			**Process Status:**	Production
External System ID:					
PDI Short Description:	A separation of at least 5 centimeters is not maintained between any RED wire line and BLACK wire lines that exit the inspectable space or are connected to an RF transmitter, or BLACK power lines, located in DOD facilities outside the continental US.				
Default Severity:	Category II			**Category:**	16P-Emanations
Reference:	NSTISSAM TEMPEST 2/95A 3 Feb 2000				
Default Vulnerability Discussion:	Failure to maintain proper separation could result in emanations of classified information.				
Default Finding Details:					
Default Recommendation:	Ensure a minimum of 5 centimeters separates any RED wire line from BLACK wire lines.				
Supplemental Information:	Overseas Locations only SIPRNet Compliance Validation				

81 PDI(s) displayed.